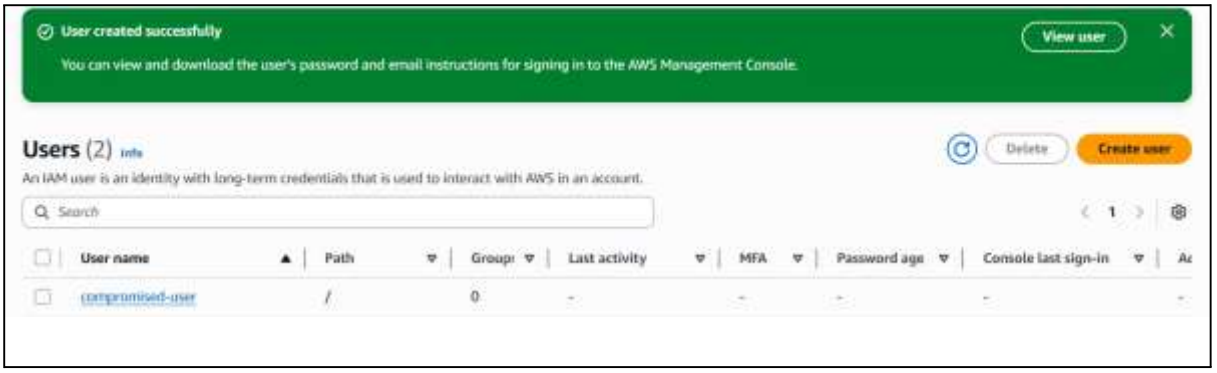
Week 8: Simulated Attack & Cloud Incident Response

Name- Samruddhi Dattu Nikam
PRN- 2124UCSF2019
Email-samruddhi.nikam_24ucs@sanjivani.edu.in

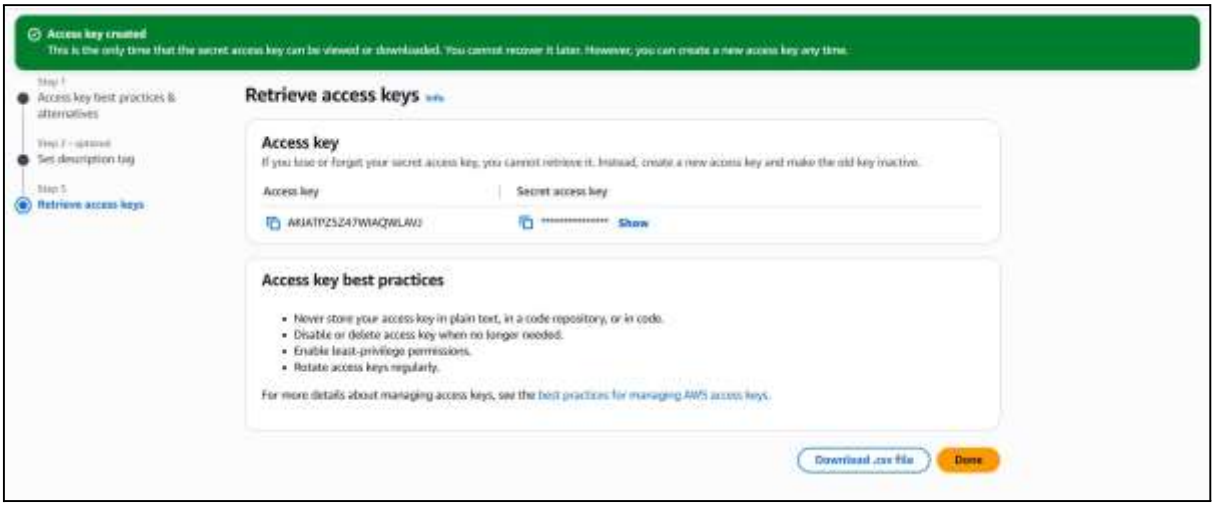
Task- 1) Simulate a compromised account scenario.
2) Respond & secure the account.
3) Document the incident response steps.

Task 1- Simulate a Compromised Account.

1) Log in to AWS Console. Go to https://aws.amazon.com, sign in to the AWS Management Console.
2) Create a test IAM user named `compromised-user` with basic permissions (e.g., Amazon S3 read access).



3) Generate **Access Keys** for the user.



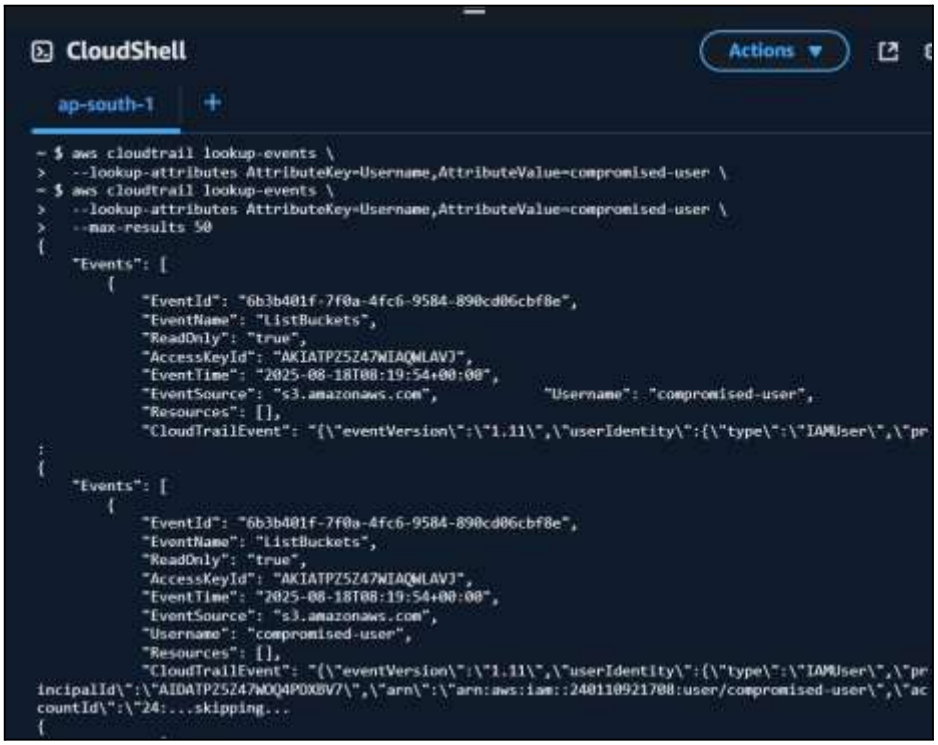
4) Share these keys intentionally with a test machine/script that attempts unauthorized AWS CLI actions (e.g., trying to delete S3 objects without permission).

Week 8: Simulated Attack & Cloud Incident Response

5) Monitor AWS CloudTrail and CloudWatch to detect unusual activity from the user account.

Task 2- Respond to the Incident.

1) Identify the Source: Go to CloudTrail → Event History. Filter by compromised-user and check the activity timeline.



2) Secure the Account: Deactivate the compromised Access Keys: aws iam update-access-key --access-key-id <ACCESS_KEY> --status Inactive --user-name compromised-user

Week 8: Simulated Attack & Cloud Incident Response

```
~ $
~ $ aws iam list-access-keys --user-name compromised-user
{
    "AccessKeyMetadata": [
        {
            "UserName": "compromised-user",
            "AccessKeyId": "AKIATPZ5Z47WIAQWLAVJ",
            "Status": "Active",
            "CreateDate": "2025-08-18T07:40:51+00:00"
        }
    ]
}
~ $ for AKI in $(aws iam list-access-keys --user-name compromised-user \
>   --query 'AccessKeyMetadata[].AccessKeyId' --output text); do
>   aws iam update-access-key --user-name compromised-user \
>     --access-key-id $AKI --status Inactive
> done
~ $ for AKI in $(aws iam list-access-keys --user-name compromised-user \
>   --query 'AccessKeyMetadata[].AccessKeyId' --output text); do
>   aws iam delete-access-key --user-name compromised-user --access-key-id $AKI
> done
~ $ aws iam delete-login-profile --user-name compromised-user
```

3) Restrict Permissions: Detach all policies from the user. Remove from any IAM group.

```
~ $
~ $ for ARN in $(aws iam list-attached-user-policies --user-name compromised-user \
>   --query 'AttachedPolicies[].PolicyArn' --output text); do
>   aws iam detach-user-policy --user-name compromised-user --policy-arn $ARN
> done
~ $ for NAME in $(aws iam list-user-policies --user-name compromised-user \
>   --query 'PolicyNames[]' --output text); do
>   aws iam delete-user-policy --user-name compromised-user --policy-name $NAME
> done
~ $ for G in $(aws iam list-groups-for-user --user-name compromised-user \
>   --query 'Groups[].GroupName' --output text); do
>   aws iam remove-user-from-group --group-name $G --user-name compromised-user
> done
~ $
```

4) Enable MFA (Multi-Factor Authentication) on the account.

Task 3- Document the Incident Response Steps.

Incident Summary:

- **Incident Type**: Simulated account compromise.
- **Impact**: Unauthorized S3 deletion attempt blocked.
- **Detection Method**: AWS CloudTrail & CloudWatch alerts.
- **Response Actions**: Access keys deactivated, permissions removed, MFA enabled.